Astérisque

J. ELSTRODT
F. GRUNEWALD
J. MENNICKE

PSL(2) over imaginary quadratic integers

Astérisque, tome 94 (1982), p. 43-60
<http://www.numdam.org/item?id=AST_1982__94__43_0>

PSL(2) OVER IMAGINARY QUADRATIC INTEGERS

by

J. ELSTRODT, F. GRUNEWALD, J. MENNICKE

-:-:-:-

1. - Introduction

This paper describes some results obtained by us on various aspects of the groups $PSL(2,\mathfrak{O})$ where $\mathfrak{O}$ is the ring of integers in an imaginary quadratic number field. Our results complement or carry further the research described in the previous papers [2], [3].

The second chapter gives some asymptotics for representation numbers of certain ternary quadratic forms. The proof uses an analysis of the spectral theory of the Laplace operator on $L^2(\Gamma\backslash\mathbb{H})$ where $\mathbb{H}$ is the 3-dimensional hyperbolic space. The group $\Gamma = PSL(2,\mathfrak{O})$ has a natural action on $\mathbb{H}$.

The third chapter describes the number of conjugacy classes of elements of order 3 in unit groups of certain integral quadratic forms. We use Siegel's theory of quadratic forms to compute the above number of conjugacy classes in terms of class numbers of binary quadratic forms.

The fourth chapter describes some computational results on the structure of certain subgroups of finite index in $PSL(2,\mathbb{Z}[i])$.

In chapter five we study the Hecke algebra in the commutator factor-group of these subgroups of finite index in $PSL(2,\mathbb{Z}[i])$. We give here some computational results which suggest a connection between the eigenspaces of the Hecke algebra and Frobenius classes in certain extension fields of $\mathbb{Q}[i]$.

2. - Asymptotic results on numbers of representations by certain special ternary quadratic forms

In this paragraph, we describe some results which are a combination of ideas of A. Schmidt and A. Thorup and our previous results [2], [3]. We collect some notation. Consider 3-dimensional hyperbolic space $\mathbb{H} \simeq PSU_2 \backslash PSL(2, \mathbb{C})$. The Poincaré upper half-space model is

$$\mathbb{H} = \{(z, r),\ z \in \mathbb{C},\ r \in \mathbb{R}^+\} .$$

The metric is given by

$$d^2s = \frac{dx^2 + dy^2 + dr^2}{r^2} , \quad z = x + iy .$$

The global distance is given by

$$\operatorname{Cos} d(P, Q) = \frac{|z-z'|^2 + r^2 + r'^2}{2rr'} = \delta(P, Q), \quad \text{say}$$

$$P = (z, r) , \quad Q = (z', r') .$$

The action of the group of orientation preserving isometries $PSL_2(\mathbb{C})$ on $\mathbb{H}$ is given by

$$X(z, r) = \left(\frac{(\bar{\gamma}\bar{z}+\bar{\delta})(\alpha z+\beta) + \alpha\bar{\gamma} r^2}{|\gamma z+\delta|^2 + r^2|\gamma|^2} , \frac{r}{|\gamma z+\delta|^2 + r^2|\gamma|^2}\right) ,$$

$$X = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in PSL_2(\mathbb{C}) .$$

The Kleinean model is defined as follows. Take a quaternary quadratic form over $\mathbb{R}$, of signature $(3, 1)$, i.e.

$$f \underset{\mathbb{R}}{\sim} -x_1^2 - x_2^2 - x_3^2 + x_4^2 .$$

Consider

$$K(f) := \{\underline{x} \in \mathbb{P}^3(\mathbb{R}),\ f(\underline{x}) > 0\} .$$

The global distance in this model is given by

$$\operatorname{Cos} d(P, Q) = \delta(P, Q) = \frac{f(\underline{x}, \underline{y})}{\sqrt{f(\underline{x})}\ \sqrt{f(\underline{y})}} ,$$

where P, Q are represented by the real homogeneous vectors $\underline{x}, \underline{y}$, respectively.

The group of isometries is $PO_4(f, \mathbb{R})$. By duality, the planes in $K(f)$ are described by the real homogeneous vectors $\underline{u} \in \mathbb{P}^3$ such that $f(\underline{u}) < 0$. A point $\underline{x}$ lies on a plane $\underline{u}$ if and only if $f(\underline{x}, \underline{u}) = 0$. For a form f with coefficients in $\mathbb{Z}$, and for points $\underline{x}$ with rational homogeneous coordinates, we introduce the notation

$$\underline{x} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}_N , \quad \text{where } x_1, x_2, x_3, x_4 \in \mathbb{Z} \text{ are relatively prime, and } f(\underline{x}) = N.$$

The coordinates x_i are uniquely determined up to a common sign ± 1, and $N \in \mathbb{Z}$ is uniquely determined. The square class of N is the spinorial norm of the reflection in $\underline{x}$.

Consider the complex quadratic field $k = \mathbb{Q}(\sqrt{-m})$, $m \in \mathbb{N}$, square-free. For simplicity, we assume $m \equiv 1, 2$ mod. 4. The adjustments for $m \equiv 3$ mod. 4 are usually obvious.

The ring of integers in k is

$$\mathfrak{O} = \{ a + b\sqrt{-m}, \ a, b \in \mathbb{Z} \} .$$

The group $\Gamma = PSL(2, \mathfrak{O}) \subset PSL(2, \mathbb{C})$ is a discrete subgroup of finite covolume. Consider the quadratic form

$$f = -x^2 - my^2 + uv .$$

The group $PO_4(f, \mathbb{Z})$ is a discrete subgroup of $PO_4(f, \mathbb{R})$ of finite covolume. There is an exact sequence describing one of the so-called exceptional isomorphisms between certain orthogonal groups and linear groups :

$$1 \longrightarrow PSL(2, \mathfrak{O}) \longrightarrow PO_4(f, \mathbb{Z}) \longrightarrow \text{cok} \longrightarrow 1 .$$

The cokernel cok is an abelian group of exponent 2, and of order $2^{w(m)+2}$, where $w(m)$ is the number of prime factors of m. The cokernel map of the above sequence can be defined via the spinorial norm.

A geometric version of the exceptional isomorphism is as follows

PROPOSITION 1. - *Consider the form*

$$f = -x^2 - my^2 + uv \;.$$

There is an isometry

$$\sigma \;:\; \mathbb{H} \longrightarrow K(f) \;, \quad \text{such that}$$

$$\begin{array}{ccc} \sigma : \left(\frac{b}{c}, \frac{\sqrt{D}}{c}\right) & \longleftrightarrow & \begin{pmatrix} b_o \\ b_1 \\ c \\ a \end{pmatrix}_D \\ b \in \mathfrak{O} & & \\ c, D \in \mathbb{N} & & b = b_o + b_1\sqrt{-m} \\ |b|^2 + D \equiv 0 \text{ mod. } c & & a, c \in \mathbb{N} \\ & & ac - |b|^2 = D \end{array}$$

The isometry is compatible with the actions of the groups $PSL(2, \mathfrak{O})$ *and* $PO_4(f, \mathbb{Z})$, *respectively*.

There is another classical model of hyperbolic 3-space : the space of binary positive definite Hermitian forms of determinant unity. Write the Hermitian form :

$$f = a|x|^2 + b\bar{x}y + \bar{b}x\bar{y} + c|y|^2 = (\bar{x}\,\bar{y})\; B\binom{x}{y} \;, \quad \text{where}$$

$$a, c \in \mathbb{R}^+ \;, \quad b \in \mathbb{C} \;, \quad ac - |b|^2 = 1 \;, \quad B = \begin{pmatrix} a & b \\ \bar{b} & c \end{pmatrix} .$$

For

$$X = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in PSL_2(\mathbb{C}) \;, \quad \text{consider}$$

$$X(0,1) = \left(\frac{\alpha\bar{\gamma} + \beta\bar{\delta}}{|\gamma|^2 + |\delta|^2}, \frac{1}{|\gamma|^2 + |\delta|^2}\right) .$$

We have

$$XX^* = \begin{pmatrix} |\alpha|^2 + |\beta|^2 & \alpha\bar{\gamma} + \beta\bar{\delta} \\ \bar{\alpha}\gamma + \bar{\beta}\delta & |\gamma|^2 + |\delta|^2 \end{pmatrix} = B \;, \quad \text{say.}$$

The mapping

$$\tau \;:\; X \text{ mod. } PSU_2 \longleftrightarrow B = XX^*$$

is a bijection which can be made into an isometry. We need the following integral version.

PROPOSITION 2. - *There is a bijection*

$$\rho \ : \ P = \left(\frac{b}{c}, \frac{\sqrt{D}}{c}\right) \longrightarrow B = \begin{pmatrix} a & b \\ \bar{b} & c \end{pmatrix}$$

$$\begin{array}{ll} b \in \mathfrak{O}, \ c, D \in \mathbb{N} & a, c \in \mathbb{N}, \ b \in \mathfrak{O} \\ |b|^2 + D \equiv 0 \ \text{mod.}\ c & ac - |b|^2 = 1 \end{array}$$

of certain points in hyperbolic 3-*space and integral binary definite Hermitian forms over* $\mathfrak{O}$ *with determinant* D .

PSL(2,$\mathfrak{O}$) -*orbits of such points correspond to* PSL(2,$\mathfrak{O}$) -*equivalence classes of Hermitian forms*.

We consider the following counting function.

$$c(n) = \# \{ X = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in PSL_2(\mathfrak{O}) \ ; \ |\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = n \} \ .$$

There is a beautiful method due to A. Schmidt and A. Thorup [8] to compute c(n).

PROPOSITION 3. (A. Schmidt and A. Thorup). - *Assume* $m \neq 1$. *We have*

$$c(n) = 2 \# \{ (x,b) \ ; \ x \in \mathbb{Z}, \ b \in \mathfrak{O}, \ x^2 + 4|b|^2 = n^2 - 4 ,$$

$$a := \frac{1}{2}(n+x) \ , \ c := \frac{1}{2}(n-x) \ , \ \begin{pmatrix} a & b \\ \bar{b} & c \end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \} \ .$$

The equivalence $\sim$ *is* PSL(2,$\mathfrak{O}$) -*equivalence of Hermitian forms*. *For* $m = 1$, *replace the factor* 2 *by* 4 .

There are some cases where the equivalence condition is trivial, because there is only one class of Hermitian forms. This holds, e.g., for $m = 1$. In these cases, c(n) is, up to a trivial factor, the number of representations of $n^2 - 4$ by the definite ternary quadratic form $g = x^2 + 4 \ |b|^2$.

If there are more than one equivalence class, then the equivalence condition in proposition 3 is very difficult to handle. There is, however, a way to produce information about the number of solutions of $g = n^2 - 4$. Introduce the counting function

$$d(n) := \# \{(x,b), \ x \in \mathbb{Z}, \ b \in \mathfrak{O}, \ x^2 + 4|b|^2 = n^2 - 4\} \ ,$$

choose a system of representatives for the equivalence classes of binary positive definite Hermitian forms over $\mathfrak{O}$ with determinant unity :

$$B_1 , B_2 , \dots \quad B_{h^*} .$$

Let $P_1, P_2, \dots \quad P_{h^*} \in \mathbb{H}$ be the points corresponding to B_i under the bijection of proposition 2. For $j = (0,1) \in \mathbb{H}$ use the identity

$$\delta(j, XP) = \frac{1}{2} \operatorname{tr}(X B X^*) \quad ,$$

where $B = \rho(P)$ corresponds to P under the above bijection. Introduce the Poincaré series

$$\theta^*(P,Q,t) := \sum_{X \in PSL(2,\mathfrak{O})} e^{-t\delta(P,XQ)} ,$$

for $P,Q \in \mathbb{H}$, $t \in \mathbb{R}^+$.

In our previous work [2], [3], we have shown

$$\lim_{t \to 0} t^2 \theta^*(P,Q,t) = \frac{4\pi}{\operatorname{vol}(\Gamma \backslash \mathbb{H})} .$$

Notice that the right hand side is independent of P, Q.

Consider the functions $\theta^*(j, P_i, t)$. By the Schmidt-Thorup theorem, we have

$$\sum_{i=1}^{h^*} \theta^*(j, P_i, t) = 2 \sum_{n=2}^{\infty} d(n)\, e^{-(tn/2)} .$$

Invoking the existence of the above limit, we conclude

$$\lim_{t \to 0} t^2 \sum_{n=2}^{\infty} d(n)\, e^{-(tn/2)} = \frac{2\pi}{\operatorname{vol}(\Gamma \backslash \mathbb{H})} h^* .$$

Invoking the Tauberian theorem of Karamata, we obtain

THEOREM 1. - Consider $k = \mathbb{Q}(\sqrt{-m})$, $m \in \mathbb{N}$, squarefree, $m \neq 1,3$. Let $\mathfrak{O} \subset k$ be the maximal order. Let h^* denote the number of $PSL(2,\mathfrak{O})$ equivalence classes of binary definite Hermitian forms over $\mathfrak{O}$ with determinant unity.

Consider the ternary definite quadratic form over $\mathbb{Z}$

$$g = x^2 + 4|b|^2 ,$$

where $|b|^2$ is the norm form in $\mathfrak{O}$. Consider the number of solutions of $g = n^2 - 4$:

$$d(n) = \# \{ (x,b) \; ; \; x \in \mathbb{Z} , \; b \in \mathfrak{O} \; , \; g = n^2 - 4 \} .$$

Then the summatory function over $d(n)$ has the asymptotic behaviour

$$\sum_{n=2}^{N} d(n) \sim \frac{\pi}{4\,\mathrm{vol}(\Gamma \backslash \mathbb{H})} \cdot h^{*} \cdot N^{2} .$$

Here $\mathrm{vol}(\Gamma \backslash \mathbb{H})$ means the covolume of $PSL(2,\mathfrak{O})$, which is

$$\mathrm{vol}\,(\Gamma \backslash \mathbb{H}) = \frac{|d|^{3/2}}{4\pi^{2}}\, \zeta_{k}(2) ,$$

d is the discriminant of k, and ζ_k is the ζ-function of k.

Although our result is special, it seems to be one of the few results which do not follow either from Siegel's theory or from the classical theory of modular functions.

Notice that the class number h^{*} can be computed using Siegel's theory of indefinite quadratic forms over $\mathbb{Z}$, because by proposition 1 and 2, it basically amounts to computing $PO_4(f, \mathbb{Z})$-orbits of

$$f = -x^{2} - my^{2} + uv = 1 ,$$

and the form f has only one class in its genus. It is likely that explicit formulas for h^{*} are in the literature, but we did not find a reference.

3. - Conjugacy classes in the extended Bianchi group

Consider the group $O_4(f, \mathbb{Z})$ for the form

$$f = -x^{2} - my^{2} + uv .$$

Since f has only one class in its genus, Siegel's theory of indefinite quadratic norms can be used to study group-theoretical properties of $O_4(f, \mathbb{Z})$. We have discussed in [1] that there are only very few conjugacy classes of involutions in $O_4(f, \mathbb{Z})$. Here we describe another similar result.

THEOREM 1. - Assume $(m, 6) = 1$.

Consider elements $X \in \Gamma = O_4(f, \mathbb{Z})$ of order 3. Any such X is a product of two involutions

$$X = \sigma\tau ,$$

where σ and τ are reflections in planes which are both in the orbit of $\sigma_2 = (0, 0, 1, -1)$. The number of conjugacy classes of elements of order 3 coincides with the number of $GL(2, \mathbb{Z})$-classes in the genus of $g = x^{2} - 3my^{2}$.

The proof of the theorem is not straightforward. Siegel's theory gives a sum of densities over the various orbits. In general, these densities are different for different orbits. It turns out that in the above special situation, this information suffices to count the number of orbits.

Notice that in the classical theory of indefinite binary forms, $SL(2, \mathbb{Z})$-classes of such forms correspond to proper equivalence classes of ideals in real quadratic number fields. A $GL(2, \mathbb{Z})$-class of forms splits into two $SL(2, \mathbb{Z})$-classes if the forms are not ambiguous, and into one $SL(2, \mathbb{Z})$-class if the forms are ambiguous.

Using more or less standard arguments from algebraic number theory, it can be shown that the number of conjugacy classes in theorem 1 can be arbitrarily large as m grows.

4. - Some commutator factor groups

The chapter gives the outcome of the explicit computation of the commutator factor group of certain subgroups of finite index in $PSL(2, \mathbb{Z}[i])$. For an ideal $\mathfrak{a} \subseteq \mathbb{Z}[i]$ put

$$\Gamma_o(\mathfrak{a}) = \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in PSL(2, \mathbb{Z}[i]) \mid c \in \mathfrak{a} \} .$$

As long as $\mathfrak{a} \neq 0$ the group $\Gamma_o(\mathfrak{a})$ is of finite index in $PSL(2, \mathbb{Z}[i])$. Using a presentation for the group $PSL(2, \mathbb{Z}[i])$ it is then an easy but tedious computation to obtain a presentation for $\Gamma_o(\mathfrak{a})$ for each particular ideal $\mathfrak{a}$. In case $\mathfrak{a}$ is a prime ideal of degree 1 the computational effort is least. From the presentation of $\Gamma_o(\mathfrak{a})$ one can then compute the structure of the commutator factor group $\Gamma_o(\mathfrak{a})^{ab}$.

We give now the result for the prime ideals $\mathfrak{p} \subseteq \mathbb{Z}[i]$ of degree 1 with norm $N(\mathfrak{p}) \leq 100$. Note that $N(\mathfrak{p}) = N(\mathfrak{q})$ implies that $\Gamma_o(\mathfrak{p})$ is isomorphic to $\Gamma_o(\mathfrak{q})$.

$N(\mathfrak{p})$	$\Gamma_0(\mathfrak{p})^{ab}$
5	$\mathbb{Z}/4\,\mathbb{Z}$
13	$\mathbb{Z}/4\,\mathbb{Z} \times \mathbb{Z}/3\,\mathbb{Z}$
17	$\mathbb{Z}/16\,\mathbb{Z}$
29	$\mathbb{Z}/4\,\mathbb{Z} \times \mathbb{Z}/21\,\mathbb{Z}$
37	$\mathbb{Z}/4\,\mathbb{Z} \times \mathbb{Z}/9\,\mathbb{Z}$
41	$\mathbb{Z}/16\,\mathbb{Z} \times \mathbb{Z}/5\,\mathbb{Z}$
53	$\mathbb{Z}/4\,\mathbb{Z} \times \mathbb{Z}/13\,\mathbb{Z}$
61	$\mathbb{Z}/4\,\mathbb{Z} \times \mathbb{Z}/15\,\mathbb{Z}$
73	$\mathbb{Z}/8\,\mathbb{Z} \times \mathbb{Z}/9\,\mathbb{Z}$
89	$\mathbb{Z}/8\,\mathbb{Z} \times \mathbb{Z}/11\,\mathbb{Z} \times \mathbb{Z}/11\,\mathbb{Z}$
97	$\mathbb{Z}/32\,\mathbb{Z} \times \mathbb{Z}/15\,\mathbb{Z}$

The first case where $\Gamma_0(\mathfrak{p})$ is infinite occurs when $N(\mathfrak{p}) = 137$. Here we find

$$\Gamma_0(\mathfrak{p})^{ab} \simeq \mathbb{Z} \times \mathbb{Z}/4\,\mathbb{Z} \times \mathbb{Z}/3\,\mathbb{Z} \times \mathbb{Z}/17\,\mathbb{Z} .$$

The cases of $\Gamma_0(\mathfrak{p})$ with infinite factor commutator group are discussed in [2], [5].

For a prime ideal $\mathfrak{p}$ put

$$\Lambda(\mathfrak{p}) = (\mathfrak{O}/\mathfrak{p})^* / \{\pm 1\}$$

where $(\mathfrak{O}/\mathfrak{p})^*$ is the multiplicative group of $\mathfrak{O}/\mathfrak{p}$. $\Lambda(\mathfrak{p})$ is a cyclic group of order $(N(\mathfrak{p})-1)/2$. There is a surjective homomorphism

$$\varphi : \Gamma_0(\mathfrak{p})^{ab} \longrightarrow \Lambda(\mathfrak{p})$$

induced by the map

$$\varphi : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \longmapsto \bar{a} .$$

This shows that the group $\Gamma_0(\mathfrak{p})^{ab}$ will be quite complicated if $N(\mathfrak{p})$ is large.

Let q be a rational prime. We put

$$A(\mathfrak{p}, q) = \Gamma_0(\mathfrak{p})^{ab} / q . \Gamma_0(\mathfrak{p})^{ab} .$$

$A(\mathfrak{p}, q)$ is a finite dimensional vector space over $\mathbb{Z}/q\,\mathbb{Z}$. We write $r(\mathfrak{p}, q)$ for its dimension.

Conjugation by the element

$$\varepsilon = \begin{pmatrix} i & 0 \\ 0 & 1 \end{pmatrix}$$

leaves the group $\Gamma_o(\mathfrak{p})$ invariant and induces an involutory automorphism $\tilde{\varepsilon}$ of $A(\mathfrak{p},q)$. If q is odd we write $A_+(\mathfrak{p},q)$ respectively $A_-(\mathfrak{p},q)$ for the +1 resp resp. -1 eigenspace of $\tilde{\varepsilon}$. We also put

$$r_+(\mathfrak{p},q) = \dim_{\mathbb{Z}/q\mathbb{Z}} A_+(\mathfrak{p},q) ,$$
$$r_-(\mathfrak{p},q) = \dim_{\mathbb{Z}/q\mathbb{Z}} A_-(\mathfrak{p},q) .$$

Clearly $r(\mathfrak{p},q) = r_+(\mathfrak{p},q) + r_-(\mathfrak{p},q)$.

For $q = 2$ we write $A_+(\mathfrak{p},2)$ for the space of invariants of $\tilde{\varepsilon}$ and $r_+(\mathfrak{p},2)$ for its dimension. Surprisingly enough $\tilde{\varepsilon}$ is a unipotent automorphism of $A(\mathfrak{p},2)$ for certain $\mathfrak{p}$.

Further we put

$$r(\mathfrak{p},\infty) = \mathrm{rk}_{\mathbb{Z}}(\Gamma_o(\mathfrak{p})^{ab})$$

for the torsion free rank of $\Gamma_o(\mathfrak{p})^{ab}$.

In the following table we give the dimensions of all $A_\pm(\mathfrak{p},q)$ for $N(\mathfrak{p}) \leq 400$ After giving the norm $N(\mathfrak{p})$ of $\mathfrak{p}$ we give the rank $r(\mathfrak{p},\infty)$. For q a rational prime we insert

$$(q,\ r(\mathfrak{p},q),\ r_+(\mathfrak{p},q))$$

if and only if $r(\mathfrak{p},q) - r(\mathfrak{p},\infty) > 0$. This leaves only finitely many q in the game.

$N(\mathfrak{p})$	$r(\mathfrak{p},\infty)$	
5	0	(2,1,1)
13	0	(2,1,1) ; (3,1,1)
17	0	(2,1,1)
29	0	(2,1,1) ; (3,1,0) ; (7,1,1)
37	0	(2,1,1) ; (3,1,1)
41	0	(2,1,1) ; (5,1,1)
53	0	(2,1,1) ; (13,1,1)
61	0	(2,1,1) ; (3,1,1) ; (5,1,1)
73	0	(2,1,1) ; (3,1,1)

$N(\mathfrak{p})$	$r(\mathfrak{p},\infty)$	
97	0	(2,1,1) ; (3,1,1) ; (5,1,1)
101	0	(2,1,1) ; (5,1,1) ; (17,1,0)
109	0	(2,1,1) ; (3,1,1)
113	0	(2,2,2) ; (7,1,1)
137	1	(2,2,2) ; (3,3,0) ; (17,2,1)
149	0	(2,1,1) ; (7,1,0) ; (37,1,1)
157	0	(2,3,2) ; (3,2,2) ; (13,1,1)
173	0	(2,1,1) ; (3,1,0) ; (43,1,1)
181	0	(2,1,1) ; (3,2,2) ; (5,1,1) ; (31,1,0)
193	0	(2,4,3) ; (3,1,1)
197	0	(2,1,1) ; (3,3,0) ; (7,1,1)
229	0	(2,1,1) ; (3,2,1) ; (19,1,1)
233	1	(2,5,3) ; (29,2,2)
241	0	(2,1,1) ; (3,1,1) ; (5,1,1) ; (19,1,1)
257	1	(2,2,2) ; (17,2,1)
269	0	(2,3,2) ; (11,1,0) ; (67,1,1)
277	1	(2,4,3) ; (3,5,5) ; (23,2,2)
281	0	(2,1,1) ; (5,2,1) ; (7,1,1) ; (11,1,0) ; (23,1,1)
293	0	(2,1,1) ; (3,2,2) ; (13,1,0) ; (73,1,1)
313	0	(2,1,1) ; (3,1,1) ; (7,1,0) ; (13,1,1) ; (37,1,1)
317	0	(2,1,1) ; (3,1,0) ; (79,1,1)
337	0	(2,3,2) ; (3,1,1) ; (7,1,1) ; (43,1,1)
349	0	(2,1,1) ; (3,1,1) ; (5,2,1) ; (29,1,1)
353	0	(2,6,5) ; (11,1,1)
373	0	(2,1,1) ; (3,1,1) ; (7,2,0) ; (31,1,1) ; (41,1,1)
389	0	(2,1,1) ; (3,2,2) ; (59,1,0) ; (97,1,1)
397	0	(2,1,1) ; (3,1,1) ; (5,1,0) ; (11,1,1) ; (19,1,1)

This table shows that the groups $\Gamma_0(\mathfrak{a})^{ab}$ can have big torsion subgroups. We do not have any general result on the nature of these torsion elements. In the next chapter we relate certain elements of $\Gamma_0(\mathfrak{a})^{ab}$ to the arithmetic of algebraic extensions of $\mathbb{Q}(i)$.

5. - Hecke operators

Let $\mathfrak{p}$ be a prime ideal of degree 1 in $\mathbb{Z}[i]$ and let ℓ be a rational prime. We shall construct now a certain algebra of endomorphisms $H(\mathfrak{p},\ell)$ of $A(\mathfrak{p},\ell)$.

Let $\mathfrak{q} = (q)$ be a nonzero prime ideal in $\mathbb{Z}[i]$. Put

$$\delta = \delta(q) = \begin{pmatrix} 1 & 0 \\ 0 & q \end{pmatrix} \in PGL(2, \mathbb{Q}(i)) .$$

Consider the diagram

$$\begin{tikzcd}
\Gamma_o(\mathfrak{p})^{ab} \arrow[d, "\mathrm{Tra}"] & & \Gamma_o(\mathfrak{p})^{ab} \\
(\Gamma_o(\mathfrak{p}) \cap \delta\, \Gamma_o(\mathfrak{p})\, \delta^{-1})^{ab} \arrow[rr, "\tilde{\delta}"] & & (\delta^{-1}\, \Gamma_o(\mathfrak{p})\, \delta \cap \Gamma_o(\mathfrak{p}))^{ab} \arrow[u, leftarrow, "\mathrm{in}"']
\end{tikzcd} .$$

Tra is the transfer map, $\tilde{\delta}$ the map induced by conjugation with δ^{-1}, in is the homomorphism induced by inclusion. We define

$$T(q) = \mathrm{in} \circ \tilde{\delta} \circ \mathrm{Tra}$$

$T(q)$ is an endomorphism of $\Gamma_o(\mathfrak{p})^{ab}$, hence $T(q)$ induces an endomorphism of $A(\mathfrak{p},\ell)$ for all ℓ .

We define now the Hecke algebra as

$$H(\mathfrak{p},\ell) = \langle T(q) \rangle \subseteq \mathrm{End}(A(\mathfrak{p},\ell))$$

the algebra generated by all these endomorphisms. The following facts are quite easy to prove.

PROPOSITION 1

1) $H(\mathfrak{p},\ell)$ is a commutative algebra
2) $H(\mathfrak{p},\ell)$ commutes with $\tilde{\varepsilon}$
3) if $\mathfrak{q} = (q) = (q')$ is a prime ideal then

$$T(q).\, v = T(q').\, v$$

for all $v \in A_+(\mathfrak{p},\ell)$.

4) The following formula holds

$$\varphi(T(q)(v)) = (\varphi(v))^{N(q)+1} \quad \text{for} \quad v \in \Gamma_o(\mathfrak{p})^{ab} .$$

The vector space $A_+(\mathfrak{p},\ell)$ and the homomorphisms $\tilde{\varepsilon}, \varphi$ are defined in § 4.

We want now to consider one dimensional eigenspaces

$$V = \langle v \rangle \subseteq A_+(\mathfrak{p}, \ell)$$

for the algebra $H(\mathfrak{p}, \ell)$. In this case we have for every prime ideal $\mathfrak{q} = (q)$

$$T(\mathfrak{q})\, v = a_{\mathfrak{q}} . v$$

with $a_{\mathfrak{q}} \in \mathbb{Z}/\ell\,\mathbb{Z}$ only depending on the ideal $\mathfrak{q}$.

Before studying specific examples we want to add the remark that it is in some cases quite easy to understand the action of $H(\mathfrak{p}, \ell)$ on certain of its eigenspaces.

PROPOSITION 2. - *Let* ℓ *be a rational prime dividing* $(N(\mathfrak{p})-1)/2$ *and let*

$$\varphi : A_+(\mathfrak{p}, \ell) \longrightarrow \Lambda(\mathfrak{p})/(\Lambda(\mathfrak{p}))^{\ell} \simeq \mathbb{Z}/\ell\,\mathbb{Z}$$

be the homomorphism induced by the φ *of the previous* § .
Let $V = \langle v \rangle \subseteq A_+(\mathfrak{p}, \ell)$ *be an eigenspace for* $H(\mathfrak{p}, \ell)$ *with* $\varphi(v) \neq 0$ *then*

$$a_{\mathfrak{q}} \equiv N(\mathfrak{q}) + 1 \mod \ell$$

for all prime ideals $\mathfrak{q}$.

Certainly $A_+(\mathfrak{p}, \ell)$ is an eigenspace for $H(\mathfrak{p}, \ell)$ if $A_+(\mathfrak{p}, \ell)$ is one dimensional. By the table given in § 4, this occurs quite often. The action of the Hecke algebra can then in many cases be computed by proposition 2. The interest is in the cases where proposition 2 does not apply.

Here we wish to discuss specifically the spaces $A_+(\mathfrak{p}, 2)$. Take for example the case $\mathfrak{p}_o = (6-11i)$, here we have $N(\mathfrak{p}_o) = 157$. From our table we find that $A_+(\mathfrak{p}_o, 2)$ is in this case a 2-dimensional vector space over $\mathbb{Z}/2\,\mathbb{Z}$.

From our definition of the Hecke operators $T_{\mathfrak{q}}$ it is obvious how to compute $T_{\mathfrak{q}}$ if $\mathfrak{q}$ is explicitly given. If one does this one finds that

$$A_+(\mathfrak{p}_o, 2) = V_o \oplus V_1$$

where V_o, V_1 are 1-dimensional eigenspaces for $H(\mathfrak{p}_o, 2)$. Take bases v_o, v_1 for V_o, V_1 then from proposition 2 it can be seen that

$$T_{\mathfrak{q}}\, v_o = 0 \qquad \forall\, \mathfrak{q} \neq \mathfrak{p} ,\ (1+i) .$$

For the other eigenvector v_1 we can only give a few examples of $a_{\mathfrak{q}}$ where

$T_{\mathfrak{q}} v_1 = a_{\mathfrak{q}} v_1$ $\qquad\qquad$ $a_{\mathfrak{q}} \in \mathbb{Z}/2\mathbb{Z}$

$\mathfrak{q}$	$a_{\mathfrak{q}}$
$1 + 2i$	1
$1 - 2i$	0
$2 + 3i$	1
$2 - 3i$	1
$1 + 4i$	1
$1 - 4i$	1
$2 + 5i$	0
$2 - 5i$	0

$\mathfrak{q}$	$a_{\mathfrak{q}}$
3	1
7	0
11	1
19	1

We want to explain now a connection of these numbers with the decomposition of prime ideals of $\mathbb{Z}[i]$ in a certain extension of $\mathbb{Q}(i)$.

Consider the polynomial

$$P_o(x) = x^3 - ix^2 - (1+i)\,x - 1 - i \ .$$

P_o is $\mathbb{Q}(i)$-irreducible and its discriminant is $2(6-11i)$. Let K_o be the field obtained by adjoining a root of $P_o(x)$ to $\mathbb{Q}(i)$. $\tilde{K}_o$ is the Galois closure of K_o. $\tilde{K}_o$ is Galois extension of $\mathbb{Q}(i)$ with Galois group

$$\mathfrak{G} = \mathfrak{S}_3 \simeq GL(2, \mathbb{Z}/2\mathbb{Z}) \ .$$

Here $\mathfrak{S}_3$ is the symmetric group on 3 elements. The field $\tilde{K}_o$ is ramified only at the primes of $\mathfrak{p}_o$ and $(1+i)$ of $\mathbb{Z}[i]$.

Let $\mathfrak{q}$ be a prime ideal of $\mathbb{Z}[i]$ with $\mathfrak{q} \nmid 2 . \mathfrak{p}_o$, and let $Fr(\mathfrak{q})$ be the Frobenius conjugacy class in $\mathfrak{G}$ corresponding to $\mathfrak{q}$. Define

$$b_{\mathfrak{q}} = \text{trace } Fr(\mathfrak{q}) \ .$$

This definition gives for every prime ideal $\mathfrak{q}$ of $\mathbb{Z}[i]$ with $\mathfrak{q} \nmid 2 . \mathfrak{p}_o$ a number $b_{\mathfrak{q}} \in \mathbb{Z}/2\mathbb{Z}$. Note that

$$b_{\mathfrak{q}} = \begin{cases} 0 \Leftrightarrow \mathfrak{q} = \mathfrak{q}_1 \cdots \mathfrak{q}_6 \text{ or } \mathfrak{q} = \mathfrak{q}_1 \mathfrak{q}_2 \mathfrak{q}_3 \text{ in } \tilde{K}_o \\ 1 \Leftrightarrow \mathfrak{q} = \mathfrak{q}_1 \cdot \mathfrak{q}_2 \text{ in } \tilde{K}_o \ . \end{cases}$$

The $\mathfrak{q}_i$ are supposed to be distinct prime ideals in the integral closure of $Z[i]$ in $\tilde{K}_o$.

Clearly $b_{\mathfrak{q}}$ can be computed as

$$b_{\mathfrak{q}} = \begin{cases} 0 \Leftrightarrow P_o(x) \text{ has one or three zeroes mod. } \mathfrak{q} \\ 1 \Leftrightarrow P_o(x) \text{ has no zero mod. } \mathfrak{q} \end{cases} .$$

We have checked for many primes ideals $\mathfrak{q}$ (in fact several hundred) of Z[i] that

$$a_{\mathfrak{q}} = b_{\mathfrak{q}} .$$

So the eigenvalues of $H(\mathfrak{p}_o, 2)$ on a certain eigenspace seem to control the decomposition of prime ideals of $\mathbb{Z}[i]$ in $\widetilde{K}_o$. Unfortunately, we cannot prove this.

We shall give now the primes $\mathfrak{p}$ of degree 1 in $\mathbb{Z}[i]$ with $N(\mathfrak{p}) \leq 400$ where $H(\mathfrak{p}, 2)$ has a nontrivial eigenspace in $A_+(\mathfrak{p}, 2)$.

An eigenspace $V = \langle v \rangle$ is called nontrivial if

$$T(q)v = v$$

for at least one prime ideal $\mathfrak{q} = (q)$ with $\mathfrak{q} \nmid 2$. If a prime $\mathfrak{p}$ is not mentioned we assert that $A_+(\mathfrak{p}, 2)$ contains only trivial eigenspaces for $H(\mathfrak{p}, 2)$.

$\underline{N(\mathfrak{p}) = 157}$

$A_+(\mathfrak{p}, 2)$ contains one nontrivial ℓ-dimensional eigenspace for $H(\mathfrak{p}, 2)$.

$\underline{N(\mathfrak{p}) = 193}$

$A_+(\mathfrak{p}, 2)$ contains one nontrivial ℓ-dimensional eigenspace for $H(\mathfrak{p}, 2)$.

Let $\widetilde{H}$ be the algebra of endomorphisms of $A_+(\mathfrak{p}, 2)$ generated by the $T(q)$ with $(q) \nmid 2\mathfrak{p}$. There is a 2-dimensional subspace in $A_+(\mathfrak{p}, 2)$ on which $\widetilde{H}$ acts by scalars.

$\underline{N(\mathfrak{p}) = 233}$

$A_+(\mathfrak{p}, 2)$ contains one nontrivial ℓ-dimensional eigenspace for $H(\mathfrak{p}, 2)$. The algebra $\widetilde{H}$ (defined as under $N(\mathfrak{p}) = 193$) has a 3-dimensional subspace of $A_+(\mathfrak{p}, 2)$ on which it acts by scalars.

$\underline{N(\mathfrak{p}) = 269}$

$A_+(\mathfrak{p}, 2)$ contains one nontrivial ℓ-dimensional eigenspace for $H(\mathfrak{p}, 2)$.

$\underline{N(\mathfrak{p}\,) = 277}$

$A_+(\mathfrak{p}\,,2)$ contains one nontrivial ℓ-dimensional eigenspace for $H(\mathfrak{p}\,,2)$.

$\underline{N(\mathfrak{p}) = 353}$

$A_+(\mathfrak{p}\,,2)$ contains one nontrivial ℓ-dimensional eigenspace for $H(\mathfrak{p}\,,2)$. The algebra $\tilde{H}$ (defined as under $N(\mathfrak{p}) = 193$) has a 3-dimensional subspace of $A_+(\mathfrak{p}\,,2)$ on which it acts by scalars.

We have described here 6 nontrivial ℓ-dimensional eigenspaces for the various $H(\mathfrak{p}\,,2)$. We give now 6 field extensions of $\mathbb{Q}(i)$ associated with these eigenspaces in the above described way.

$P(x)$	$\Delta(P(x)$	$N(\Delta(P(x))$
$x^3 - i\,x^2 - (1+i)\,x - 1 - i$	$4.(6-11i)$	16.157
$x^3 - i\,x^2 - (1+2i)\,x + i$	$4.(-7-12i)$	16.193
$x^3 - (1+i)\,x^2 + 2i\,x - 2i$	$4.(13-8i)$	16.233
$x^3 - x^2 + (1-i)\,x - 1 - i$	$4.(10-13i)$	16.269
$x^3 - (1+i)\,x^2 - (2-i)\,x - 1 + i$	$4.(-14+9i)$	16.277
$x^3 - i\,x^2 - (1+i)\,x - 1$	$-17 - 8i$	353

For each of the polynomials P in this list let $\tilde{K}_P$ be the associated Galois extension of $\mathbb{Q}(i)$. $\tilde{K}_P$ has Galois group $GL(2\,,\mathbb{Z}/2\mathbb{Z})$ over $\mathbb{Q}(i)$. Take $V = \langle v\rangle$ the nontrivial eigenspace for $H(\mathfrak{p}\,,2)$ in $A_+(\mathfrak{p}\,,2)$ with $\mathfrak{p} = \frac{1}{2}(\Delta(P(x)))$ or $\mathfrak{p} = (\Delta(P(x)))$. Then in each case we have checked for many primes $\mathfrak{q} = (q) \nmid 2\mathfrak{p}$ of $\mathbb{Z}[i]$ that

$$a_{\mathfrak{q}} = \mathrm{Trace}\;Fr(\mathfrak{q})$$

where $T_{(q)}\,v = a_{\mathfrak{q}}\,v$.

There remains the question of how we have singled out the above extensions of $\mathbb{Q}(i)$ from the many extensions with Galois group $S_3 \simeq GL(2\,,\mathbb{Z}/2\mathbb{Z})$.

We make the following definition.

DEFINITION. - Let $\mathfrak{p}$ be a prime ideal of degree 1 in $\mathbb{Z}[i]$ with $\mathfrak{p} \nmid 2$. A cubic polynomial $P(x) = x^3 + a_1x^2 + a_2x + a_3$, $a_1, a_2, a_3 \in \mathbb{Z}[i]$, is said to be of type $\mathfrak{p}^1$ iff

1) $P(x)$ is irreducible over $\mathbb{Q}(i)$,

2) the discriminant $\Delta(P(x))$ is only divisible by $\mathfrak{p}$ and $(1+i)$,

3) $P(x)$ has a double but no triple zero mod. $\mathfrak{p}$,

4) $1+i$ divides $\Delta(P(x))$ exactly to an even power.

These conditions can also be interpreted as a certain ramification behaviour of $\mathfrak{p}$ and $(1+i)$ in the Galois closure of $P(x)$.

We have carried out an extensive search for polynomials of type $\mathfrak{p}^1$. For each of the polynomials we found we have also found a corresponding eigenspace of $H(\mathfrak{p}, 2)$ in $A_+(\mathfrak{p}, 2)$. For every eigenspace we have also found a corresponding polynomial.

At other torsion primes $\ell \neq 2$ we have also analysed the eigenspaces of $H(\mathfrak{p}, \ell)$ in $A_+(\mathfrak{p}, \ell)$. We have found similar phenomena.

Finally we would like to mention the case $\mathfrak{p} = (13 + 12i)$, $N(\mathfrak{p}) = 313$. Here $A_+(\mathfrak{p}, 37) = \mathbb{Z}/37\mathbb{Z}$ is an eigenspace for $H(\mathfrak{p}, 37)$. We give a few examples of eigenvalues.

$\mathfrak{q}$	$a_{\mathfrak{q}}$
1 + 2i	17
1 - 2i	3
2 + 3i	18
2 - 3i	25
1 + 4i	36
1 - 4i	22

$\mathfrak{q}$	$a_{\mathfrak{q}}$
3	4
7	1
11	1
19	1
23	3
21	1

Here $a_{\mathfrak{q}}$ is the eigenvalue of $T(\mathfrak{q})$ on $A_+(\mathfrak{p}, 37)$. It would be interesting to find a field $K \geq \mathbb{Q}(i)$ with Galois group $GL(2, \mathbb{Z}/37\mathbb{Z})$ such that

$$a_{\mathfrak{q}} = \text{Trace}\,(Fr(\mathfrak{q})).$$

for $\mathfrak{q} \nmid 37.\mathfrak{p}$. If such a field exists it could of course not be the 37-division field of an elliptic curve defined over $\mathbb{Q}(i)$. No such example seems to be known.

-:-:-:-

REFERENCES

[1] J. ELSTRODT, F. GRUNEWALD, J. MENNICKE, *Spectral theory of the Laplacian on* 3-*dimensional hyperbolic space and number theoretic applications*, to appear.

[2] J. ELSTRODT, F. GRUNEWALD, J. MENNICKE, *On the group* PSL(2, $\mathbb{Z}[i]$), Journées Arithmétiques 1980, LMS Lecture Notes 56 (1982), 255-283, ed. J. V. Armitage.

[3] J. ELSTRODT, F. GRUNEWALD, J. MENNICKE, *Discontinuous groups on* 3-*dimensional hyperbolic space*, Analytical Theory and arithmetic applications, to appear, Uspehi Mat. Nauk.

[4] F. GRUNEWALD, H. HELLING, J. MENNICKE, SL(2,$\mathfrak{O}$) *over complex quadratic numberfields*, Algebra i Logika 17, 512-580 (= Algebra and Logic 17 (1978), 332-382).

[5] F. GRUNEWALD, J. MENNICKE, $SL_2(\mathfrak{O})$ *and elliptic curves*, Manuscript Bielefeld (1978).

[6] F. GRUNEWALD, J. MENNICKE, *Some* 3-*manifolds arising from* $PSL_2(\mathbb{Z}[i])$, Archiv für Mathematik 35 (1980), 275-291.

[7] F. GRUNEWALD, J. SCHWERMER, *A non vanishing result for the cuspidal cohomology of* SL(2) over imaginary quadratic integers, Math. Annalen 258 (1981), 183-200.

[8] A. SCHMIDT, A. THORUP, Manuscript, Copenhagen (march 1982).

-:-:-:-

J. ELDTRODT
Math. Institut der
Universität Münster
Einstein-Str. 62
4400 MÜNSTER
BRD

F. GRUNEWALD
Math. Institut der
Universität Bonn
Wegeler Straße 10
5300 BONN 1
BRD

J. MENNICKE
Fakultät für Mathematik
Universität Bielefeld
Universitätsstraße 1
4800 BIELEFELD 1
BRD